

VISIT...

LANZAROTE
Caliente.COM

Implanted Computer Chips

By: Gabrielle Olivera

Women in Technology

Bradley University

753 W. Wonderview dr.

Dunlap, IL 61525

1-309-243-5598

golivera@bradley.edu

ABSTRACT

This paper discusses the future of RFID technology and the possible social implications it may bring about.

Categories and Subject Descriptors:

K.4.4 [Computers and Society]: Electronic Commerce-*Electronic Data Exchange, and Security.*

General Terms:

Security and Human Factors.

Key Words:

Radio Frequency Identification (RFID)

1. INTRODUCTION:

Imagine the Future. Flying cars that run on hydrogen fuel zoom past. Food is taken like daily medication, encapsulated in pills. Births of children are monitored and restricted as space becomes more limited. Men and women dash down the streets, having conversations with the cell phone chip implanted in their ears. Another computer chip is implanted in their arms to keep track of their name, birth date, credit card information, criminal record, and home address. Another chip, implanted in their nervous system, will allow movies and television to be networked directly into their minds. The same chip allows advertisers to play commercials in a person's skull every time the chip is active.

This view of the future is not as radical as it seems. Although flying cars might be an extreme concept, food pills probably not likely, and monitored births sound like a conspiracy theory, implanted chips are not only a realistic prediction, but already exist. The VeriChip, created by Applied Digital, is the first implantable microchip, and has already been implanted in approximately 2,000 people worldwide. Presently the VeriChip only keeps track of a person's medical information. The size of a grain of rice, the VeriChip is implanted in its buyer's arm in a procedure that involves a couple of minutes, antiseptic swab, a

local anesthetic, an injection and a Band Aide (Grossman 84). However this new technology frightens many journalists, intellectuals, and even some of technologies most loyal supporters. The makers of the VeriChip are not concerned, however; why should they be? Historically every technological-advancement has been viewed by the morally conscious, the conservatives, and the cynical as being frightening. But yet somehow, that technology still came, still prevailed, and still became a way of life. The technology itself does not frighten most. Although religious leaders of more conservative sects might argue that chips might disrupt the Creators' initial purpose for mankind, most see implanted chips as threatening for the same reason implanted chips are seen as exciting to their supporters: their multiple uses. Implanted chips can be used in entertainment to directly convey movies, television programs, and video games directly in the nervous system. They can be used in hospitals, to keep track of a person's medical records, heartbeat, blood pressure, and temperature. They can be used in law enforcement, to track ex-convicts, parolees, and multiple offenders. They can be used in security, so companies know their employees from possible thieves or hackers. The uses seem endless, so the fear is endless. These computer chips won't be immune to viruses, hackers, break downs, or ill usage. Do human beings really want a computer chip, prone to the same dysfunction as their lap tops at home, to be inserted inside their bodies? What if something goes wrong? Do they really want their information floating about in radio waves, easy to intercept by anyone who might want it? Do they want to be tagged like cows, to be tracked, and monitored, by whomever so wishes? In the end the threat these chips bring to a person's civil rights, privacy, and humanity out weigh their technological advantages.

2. HISTORICAL AND MODERN USES:

The VeriChip is based off a technology that is at least sixty years old. RFID (Radio Frequency Identification) has existed since the 1940s, used in a device called the IFF (Identification Friend or Foe) system. British Pilots depended on the IFF systems in their planes to distinguish between their own planes and those belonging to German forces (Crispo 62). Now reduced to the size of a grain of rice, RFID tags are used in "electronic article surveillance" in libraries. They are used to aid processes for supply chain handling, such as loading, docking, etc. Automatic payment is noted as one of RFID's most attractive uses. The chip has been inserted into "smart cards" used to automatically charge the user once he/she passes a certain RFID tracking point (63). The chip can also be used for security purposes. ID cards carrying chips could identify their carriers and distinguish an employee from a non-employee more effectively than a manual checkpoint. Another modern use of the chip is in tracking livestock and pets.

These chips are usually “injected beneath the skin” of an animal. Crispo and his colleagues note later that RFID have also been used to track people, such as medical patients, or the elderly, but these chips are not injected, but placed into wristbands. “Clothes, packaged foods, medical bottles, rental cars, airline baggage, library books, banknotes, driver’s licenses, employee badges and even surgical patients,” Crispo, Rieback, and Tannenbaum list as other items that have been tagged by the RFID (64).

However vast the uses are, RFID tags are not commonly used. They have only begun just recently to make headlines, as Wal-Mart, Tesco, and the US Department of Defense have released plans to begin to use them (Want 26). “So why has it taken over 50 years for this technology to become mainstream?” Roy Want of Intel Research asks, “The primary reason is cost,” (25). Especially when considering inserting the RFID onto consumer products such as clothes, packaged foods, or other products, cost is very important. The simplest of RFID tags can be as expensive as 13 cents a tag. That might not sound like much, but compared to bar codes which cost nothing since they are printed on the label, the price adds up. On lower priced items, such as candy, canned foods, etc, where the products could be under a dollar themselves a 13-cent tag could either reduce profit for the producer, or increase the cost for the consumer (32). Want predicts that RFID tags will begin to be seen more widely in higher-priced items. Such as in \$100-television-sets, the 13 cent difference between one TV-set and another would not affect a customer’s decision to buy.

One of these high-priced items is the 200-dollar VeriChip, which Applied Digital hopes will be used in over 200 hospitals by 2007 (Fonda 97). The VeriChip, is a RFID chip that is injected in a patient’s skin. Its current use in hospitals is to track its host’s medical information, including their personal information, such as their names, addresses, insurance information, and medical history. “That could be lifesaving in an emergency cutting the likelihood of medical errors for accident victims [...]” Fonda writes. Identification of patients is a major problem in hospitals. Many patients are rushed to hospitals, too disoriented or traumatized to remember their medical information. Doctors are then forced to act without information that might save a patient from further damage. Such information as allergies to certain anesthesia or history of heart attacks or high blood pressure could severely change the way a doctor would treat an emergency victim. Dr. John Halamka MD uses these reasons to justify why he allowed himself to be “chipped.”

“For some implanted health care identifiers might quickly prove useful. For patients with Alzheimer’s disease who wander away from home, an identifier that enables caregivers to identify nonverbal or confused patients and determine their health care preferences could be very desirable. However inserting a chip into a patient who is incapable of giving consent raises ethical issues,” (332).

3. VULNERABILITIES AND POLITICS:

The chips vulnerability to attack raises a significant privacy concern. “Since its invention the 1940s, RFID has been an obvious target for abuse,” states Crispo, Rieback, and Tannenbaum (62). They continue by explaining that RFID vulnerability is due to its wireless capabilities. “Wireless

identification is a powerful capability, and RFID reveals both a physical object’s nature and location.” This proved both useful and detrimental to the British pilots who used IFF technology during World War II. Although they were able to track their own planes through this radar system, they shared this capability with German hackers. Germans were able to track allied forces and shoot them down using their own radars. The Allied forces would throw strips of aluminum foil into the sky to set off their own systems. This kept the German radar from accurately tracking an IFF system, and saved Allied pilots from harm. Using recordings of previous Allied IFF responses and replaying them, Germans could trick Allied forces into thinking that German planes were friends not foes. Germans also created a “counter-IFF jamming radar” that administrated “denial of service,” commands to make it more difficult for Allied forces to tell their planes from German planes (64-65).

Many of these weaknesses still exist. Crispo, Rieback, and Tannenbaum list off modern, sniffing, tracking, spoofing and replay attack-methods (65-66). These methods will allow hackers to easily disrupt or steal information from any RFID tag, including the VeriChip. What makes it so vulnerable is how it works. Radio waves are sent wirelessly and therefore have no clear path, and no way of distinguishing a reader from another reader. Therefore anyone with a RFID reader will be able to read any RFID tag. Another problem caused by these invisible channels is “[...] we don’t know when communication is occurring” (Want 31). A chip which holds its host’s personal, private information could communicate with any reader at any time without its host knowing. This does raise a significant privacy concern: if anyone at anytime within a certain distance can read a host’s information from his/her implanted chip, then what is going to stop those people from misusing the information to rob, exploit, or in other ways harm the owner? Want suggests political laws or regulations to monitor RFID use, although he never mentions the VeriChip specifically (32).

“Currently, no laws regulate tag use,” Want explains. He predicts that the chips will be unsuccessful if companies that use RFID technology do not at least publicly announce their own set of regulations to guarantee customer information security. “VeriMed is tamper-proof, loss-proof, and, completely under the patient’s control,” Applied Digital assures its customers on its website www.verichipcorp.com (Privacy Policy 1). VeriMed is the patented VeriChip that is being used now in 58 hospitals, to track medical information. As of now, the chip is completely optional. Applied Digital is not content with their VeriChip being used in hospitals only. On their site they list six separate uses for RFID technology: “infant protection”, “wander prevention”, “access control”, “patient identification”, “asset tracking”, and “vibration monitoring.” Although their proposed solutions do not always involve an implanted VeriChip, Applied Digital does not hide the fact that their new technology knows no limits. Scott Silverman, CEO of Applied Digital, has expressed hopes to sell the chip to the Pentagon, CIA, and FBI (Fonda 97). Applied Digital does not limit them to even this country. When they had problems getting the FDA to approve their VeriChips right away, Applied Digital began to sell their chips overseas.

4. ETHICS:

Applied Digital’s VeriGuard system is already being used in various facilities throughout the U.S. VeriGuard is a similar

system to VeriMed. These chips instead hold access information that allows guards to access high security vaults or safes, with no need for an ID or smart card. "The chip is under your skin," John Procter spokes person for VeriChip explains, "you can't lose it. It can't be forgotten at home, and very likely it can not be taken away from you without someone being extremely motivated" (Zwin 1). So far businesses do not force their security guards to "get chipped." However, as the technology grows to be a more attractive security resolution, businesses might have to devise ways to persuade their employees to get implanted. Especially since, the VeriGuard chip does not in any way benefit their hosts. In a way, it dehumanizes its implantee, making them nothing less but walking keys.

Implanted tracking devices for the elderly or ex-convicts are also dehumanizing for similar reasons. In a sense, they are no different than the implanted RFID chips that are implanted in livestock today.

It seems that U.S. citizens are not regarding their privacy with the same regard they used to. Perhaps they should not be so eager to allow anyone to know their precise location at any time. Even if citizens were only tracked by the U.S. government itself, citizens can not be assured of their safety. Extreme power is often times as corrupting as it is useful.

5. CHIPS IN THE NERVOUS SYSTEM:

Technological eccentric Kevin Warwick made news late 2002 when he announced that he was having a RFID chip implanted directly to his nervous system (Grossman 57). The chip, Kevin hoped, would stimulate his nerves to produce small movements and sensations. If all went well, Warwick planned to implant a chip to communicate with his in his wife's nervous system. "If I move my finger, she'll feel something. We'll be closer than anybody's been before, nervous system to nervous system." Chips that simulate reality: what a terrifying concept? Reality exists only in the communication between human senses and their brains. If chips can induce the nervous system to feel, they could induce the eyes to see, the ears to hear, the tongue to taste, and the nose to smell, what then would separate simulated computer reality from natural reality? Sure such an innovation does have its uses. Movies and television shows could become as real as the most elaborate dreams. Video games would become especially exciting, allowing gamers to feel, hear, see, taste, and smell the game-world as a character, rather than only be able to move a character through a controller. However, do human beings need their entertainment to be so real?

In 1965, the New York Times published a frightening article discussing the work of Professor Jose Manuel Rodriguez Delgado (1). Delgado pioneered an implanted Radio Frequency technology that can actually control certain functions in the brain. He demonstrated his invention on a charging bull, that he was able to control using a simple radio frequency remote control. "[...] he has been able to 'play' monkeys and cats like little electronic toys that yawn, hide, fight, play, mate and go to sleep on command," reports John A. Osmundsen. Through his experiments, Delgado discovered that monkeys would learn how to control each other using remote buttons. When he stimulated monkeys to aggressive behavior, he found that they intelligently selected to take out their anger on enemy monkeys, rather than friendly ones. He also discovered that monkeys, cats, and other animals, which he

'programmed' to perform patterns of behavior would do the same pattern every time he repeated the stimuli he used the first time, but they would modify their route if there were any obstacles in their paths. Delgado wanted to use his technology to help learn something about how the brain works, but the potential of his inventions scared many of his colleges. Mind control has shadowed many Science Fiction themes from *Twilight Zone* episodes to modern movies and novels. Yet very few scientists, corporations, or politicians have discussed mind control as a possibility, at least not publicly. Delgado in his time and still is regarded as a mad man. Certainly, his experiments did allow incite to the workings of the mind; however, once Delgado began discussing the possibility of controlling armies with his device, the professor seemed more like a Bond villain than a scientist.

6. CONCLUSION AND PREDICTIONS:

Implanted radio frequency chips controlling the mind is the worse possible use for this technology, and the least probable. The technology can be and has already been invented, but very few will implement it. No industrialized nation will currently allow such a technology, because of its clear inhuman consequences. RFID chips for the nervous system are also not likely to catch on soon. Not only does a chip in the nervous system promote many of the same fears as does the thought of mind control, price continues to be an issue. Current VeriChips are priced at \$200 (Fonda 97), and are not covered by insurance. Chips for the nervous system would probably be more expensive, since the medical procedure to insert them would be more delicate, than that of the VeriChip. Even the VeriChip's price will limit its consumer range. Very few can spend \$200 for an uncertain technology, especially when its current use (to archive medical information or to allow secure access) benefits hospitals and businesses more than each individual host. Hospitals that use VeriMed technology are more likely to convince patients or families of patients (in the case of infants, Alzheimer victims, or other patients that are not completely coherent) to wear wrist bands or carry around smart cards with RFID technology than implant a chip.

But be warned, as prices of RFID technology continues to fall, RFID technology will grow more prevalent. Within the next decade, products from clothing, to food products, to furniture, to appliances will be tracked by some form of RFID. What about human tracking? Whether or not the VeriChip or other implanted RFID technologies will succeed depends on the will of citizens of United States, Great Britain, Japan, and other world powers. Citizens must consider their dignity, their rights, and remember that an implanted chip can not be removed, it can not be monitored, and it can not be completely safe. History shows that governments take advantage of the overly naïve. Trust can be patriotic, but it also can cripple. Asking questions is important and intelligent. If a technology can exploit, can control, and steal the independence human beings historically fought for, it will. Implanted chips have the potential to allow un-warranted tracking, users to access data without permission, even to control the mind. Only human resistance prevents this technology from assuming its full potential. And as long as citizens can continue to resist to be implanted with a chip like livestock or to be labeled like an item of clothing, they must.

7. REFERENCES:

- [1] Crispo, Brian, Melanie R. Rieback, and Andrew S. Tannenbaum. "The Evolution of RFID Security." IEEE Pervasive Computing Magazine 5. 1 (2005), 62-69
- [2] Fonda, Darren. "Biochips." Times (24, October 2005), 97.
- [3] Grossman, Lev. "Meet the Chipsons." Times (11, March 2002.) 56-57.
- [4] Halamka, Dr. John. "Straight from the Shoulder," The New England Journal of Medicine 353:331-333. (28, June 2005), 331-333.
- [5] Osmundsen, John. "'Matador' with a Radio Stops Wired Bull Modified Behaviour in Animals the Subject of Brain Study." New York Times (17 May 1965).
<<http://www.wireheading.com/matador.html>>
- [6] Want, Roy. "An Introduction to RFID Technology." IEEE Pervasive Computing Magazine 5. 1 (2005), 25-33.
- [7] VeriChip Corporation. 2006. VeriChip Corporation. 10, April 2006. <www.verichipcorp.com>
- [8] Zwin, Erin. "Security System Gets Under Skin with Embedded Access Chips." Security System News (16, February 2006),
<<http://www.verichipcorp.com/news/1140111202>>